

NETWORK POLICY SERVER INSTALLATION

SERVER 2012

Dashboard

- Local Server
- All Servers
- AD CS
- AD DS
- DNS
- File and Storage Services ▸
- IIS
- Remote Access

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

- Add Roles and Features
- Remove Roles and Features
- Add Servers
- Create Server Group
- Server Manager Properties

ROLES AND SERVER GROUPS

Roles: 6 | Server groups: 1 | Servers total: 1

Hide



Before you begin

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

< Previous

Next >

Install

Cancel



Select installation type

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

- Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.
- Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel



Select destination server

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

Name	IP Address	Operating System
testserver.testserver.com		Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

Select server roles

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
- Hyper-V
- Network Policy and Access Services**
- Print and Document Services
- Remote Access (Installed)
- Remote Desktop Services

Description

Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

< Previous

Next >

Install

Cancel



Add Roles and Features Wizard



Add features that are required for Network Policy and Access Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- ▾ Remote Server Administration Tools
 - ▾ Role Administration Tools
 - [Tools] Network Policy and Access Services Tools

Include management tools (if applicable)

Add Features

Cancel



Select server roles

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
- Hyper-V
- Network Policy and Access Services**
- Print and Document Services
- Remote Access (Installed)
- Remote Desktop Services

Description

Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

< Previous

Next >

Install

Cancel



Select features

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

Select one or more features to install on the selected server.

Features

- .NET Framework 3.5 Features (1 of 3 installed)
- .NET Framework 4.5 Features (4 of 7 installed)
- Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BitLocker Network Unlock
- BranchCache
- Client for NFS
- Data Center Bridging
- Direct Play
- Enhanced Storage
- Failover Clustering
- Group Policy Management (Installed)
- IIS Hostable Web Core
- Ink and Handwriting Services (Installed)

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous

Next >

Install

Cancel



Network Policy and Access Services

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

Network Policy and Access Services allows you to define and enforce policies for network access authentication, authorization, and client health using Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).

Things to note:

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.
- NAP helps you ensure that computers connecting to the network are compliant with organization network and client health policies. After installing NPS using this wizard, you can configure NAP from the NPAS home page using the NPS console.

< Previous

Next >

Install

Cancel



Select role services

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

Select the role services to install for Network Policy and Access Services

Role services

<input checked="" type="checkbox"/> Network Policy Server
<input type="checkbox"/> Health Registration Authority
<input type="checkbox"/> Host Credential Authorization Protocol

Description

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

< Previous

Next >

Install

Cancel

DESTINATION SERVER
testserver.testserver.com

Add Roles and Features Wizard



Add features that are required for Health Registration Authority?

You cannot install Health Registration Authority unless the following role services or features are also installed.

- ▾ Web Server (IIS)
 - ▾ Management Tools
 - ▾ IIS 6 Management Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools

Include management tools (if applicable)

Add Features

Cancel

Policy and Access Services



Description

Health Registration Authority (HRA) issues health certificates to NAP client computers that are compliant with network health requirements.

< Previous

Next >

Install

Cancel



Select a role service

DESTINATION SERVER
testserver.testserver.com

Add Roles and Features Wizard

Add features that are required for Host Credential Authorization Protocol?

You cannot install Host Credential Authorization Protocol unless the following role services or features are also installed.

- ▾ Web Server (IIS)
 - ▾ Web Server
 - ▾ Security
 - Basic Authentication
 - Digest Authentication

Include management tools (if applicable)

Network Policy and Access Services

Description

Host Credential Authorization Protocol (HCAP) allows you to integrate your Microsoft Network Access Protection (NAP) solution with Cisco Network Access Control. When you deploy HCAP with Network Policy Server (NPS) and NAP, NPS can perform the authorization of Cisco Network Access Control clients.

Select role services

DESTINATION SERVER
testserver.testserver.com

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Confirmation

Results

Select the role services to install for Network Policy and Access Services

Role services

- Network Policy Server
- Health Registration Authority
- Host Credential Authorization Protocol

Description

Host Credential Authorization Protocol (HCAP) allows you to integrate your Microsoft Network Access Protection (NAP) solution with Cisco Network Access Control. When you deploy HCAP with Network Policy Server (NPS) and NAP, NPS can perform the authorization of Cisco Network Access Control clients.

< Previous

Next >

Install

Cancel

Certification Authority

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Network Policy and Acces...

Role Services

Certification Authority

Authentication Requir...

Confirmation


Results

Health Registration Authority (HRA) requires that at least one Certification Authority (CA) be associated with it.

- Use the local CA to issue health certificates for this HRA server.
There is an existing CA on this computer. If you choose to use it, it will be dedicated to issuing health certificates.
- Use an existing remote CA.
If you choose to use an existing CA it should be one dedicated to issuing health certificates.

Select...

- Select a CA later using the HRA console.

 You will not be able to issue health certificates to NAP client computers until this CA is configured.

< Previous

Next >

Install

Cancel



Authentication Requirements

DESTINATION SERVER
testserver.testserver.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Network Policy and Acces...
- Role Services
- Certification Authority
- Authentication Requir...**
- Confirmation
- Results

Health Registration Authority can be configured to ensure that only users authenticated to the domain can get health certificates.

Do you want to require that users be authenticated in order to get a health certificate?

- Yes, require requestors to be authenticated as members of a domain. (recommended)
This option is only available when the computer is joined to a domain.
- No, allow anonymous requests for health certificates.

< Previous

Next >

Install

Cancel

Confirm installation selections

DESTINATION SERVER
testserver.testserver.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Network Policy and Acces...
- Role Services
- Certification Authority
- Authentication Requir...
- Confirmation**
- Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Network Policy and Access Services
 - Health Registration Authority
 - Host Credential Authorization Protocol
 - Network Policy Server
- Remote Server Administration Tools
 - Role Administration Tools
 - Network Policy and Access Services Tools
- Web Server (IIS)
 - Management Tools
 - IIS 6 Management Compatibility

[Export configuration settings](#)
[Specify an alternate source path](#)

Installation progress

[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Network Policy and Acces...](#)[Role Services](#)[Certification Authority](#)[Authentication Requir...](#)[Confirmation](#)[Results](#)

View installation progress

 Feature installation

Installation succeeded on testserver.testserver.com.

Network Policy and Access Services

- Health Registration Authority

- Host Credential Authorization Protocol

- Network Policy Server

Remote Server Administration Tools

- Role Administration Tools

 - Network Policy and Access Services Tools

Web Server (IIS)

- Management Tools

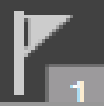
 - IIS 6 Management Compatibility

 - IIS 6 Scripting Tools



You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)[< Previous](#)[Next >](#)[Close](#)[Cancel](#)



Manage

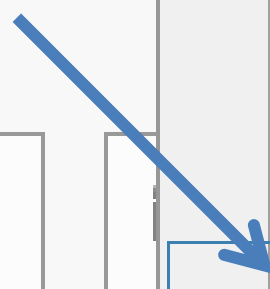
Tools

View

H

- Active Directory Administrative Center
- Active Directory Domains and Trusts
- Active Directory Module for Windows PowerShell
- Active Directory Sites and Services
- Active Directory Users and Computers
- ADSI Edit
- Certification Authority
- Component Services
- Computer Management
- Connection Manager Administration Kit
- Defragment and Optimize Drives
- Disk Cleanup
- DNS
- Embedded Lockdown Manager
- Event Viewer
- Group Policy Management
- Health Registration Authority
- Internet Information Services (IIS) Manager
- iSCSI Initiator
- Local Security Policy
- Microsoft Azure Services
- Network Policy Server

1



File Action View Help

← → [Refresh] [Help] [Print]

NPS (Local) [Refresh] [Help] [Print]

- ▶ RAD
- ▶ Policies
- ▶ Network Access Protection
- ▶ Accounts
- ▶ Templates

Import Configuration

Export Configuration

Start NPS Service

Stop NPS Service

Register server in Active Directory

Properties

View ▶

Help

ver (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

ation

enario from the list and then click the link below to open the scenario wizard.

NETWORK ACCESS PROTECTION (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

[Configure NAP](#) [Learn more](#)

Advanced Configuration

Templates Configuration

< ||| >

Network Policy Server

File Action View Help


← → [Icons]

NPS (Local)

- ▷ RADIUS Clients and Servers
- ▷ Policies
- ▷ Network Access Protection
- ▷ Accounting
- ▷ Templates Management

NPS (Local)

Getting Started

 Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.


Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy configuration of NAP-capable client computers with health policy can be placed on a restricted

 [Configure NAP](#)

Advanced Configuration

Templates Configuration

Network Policy Server

To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.

Do you wish to authorize this computer to read users' dial-in properties from the testserver.com domain?


OK Cancel



- NPS (Local)
- > RADIUS Clients and Servers
- > Policies
- > Network Access Protection
- > Accounting
- > Templates Management

NPS (Local)

Getting Started

 Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP) ▼

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, the configuration of NAP-capable client computers before the configuration with health policy can be placed on a restricted network.

 [Configure NAP](#)

Advanced Configuration

Templates Configuration

Network Policy Server [X]

This computer is now authorized to read users' dial-in properties from domain testserver.com.

To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/NPS Servers Group in that domain.

OK



- NPS (Local)
- ▷ RADIUS Clients and Servers
- ▷ Policies
- ▷ Network Access Protection
- Accounting
- ▷ Templates Management

NPS (Local)


Getting Started



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Standard Configuration


Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP) 

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

 [Configure NAP](#)

 [Learn more](#)

Advanced Configuration

Templates Configuration